JOURNAL OF ALGEBRA 47, 313–322 (1977)

Erzeugbarkeit dyadischer orthogonaler Gruppen durch Spiegelungen

H. REITER

Department of Mathematics, Universität Mainz, Mainz, Germany

Communicated by B. Huppert

Received June 9, 1976

Vor ungefähr zehn Jahren haben O'Meara und Pollak in zwei Arbeiten [2] und [3] gezeigt, daß bis auf einige Ausnahmen die orthogonale Gruppe eines unimodularen Gitters über einem dyadischen lokalen Körper der Charakteristik Null von Spiegelungen erzeugt wird. Im folgenden soll diese Frage für beliebige diskrete Bewertungsringe mit Restklassencharakteristik zwei untersucht werden. Dabei wird im Beweis von Satz 1.1 eine Idee verwendet, die sich schon bei Kneser in [1] findet.

1. Erzeugung der orthogonalen Gruppe durch Spiegelungen und verallgemeinerte Eichlertransformationen

Sei A ein diskreter Bewertungsring mit Quotientenkörper B und Primelement p und es gelte $2 \in pA$. Sei U ein endlichdimensionaler B-Vektorraum mit quadratischer Form q und E ein Gitter in U. Ist $b\colon U \times U \to B$ mit $b(x, y) = q(x + y) - q(x) - q(y)$ die zu q gehörige Bilinearform so wollen wir voraussetzen:

$$b(E, E) \subseteq A \text{ sowie} \tag{1}$$

E ist bezüglich b ein unimodulares Gitter, d.h. die Abbildung $l_E\colon E \to E^* = \mathrm{Hom}(E, A)$ mit $l_E(x)(y) = b(x, y)$ für alle $x, y \in E$ ist ein Isomorphismus. (2)

Ist für $h \in E$ $q(h) \notin pA$, so ist $s_h\colon E \to E$ mit $s_h(x) = x - (b(h, x)/q(h))h$ eine orthogonale Transformation, die Spiegelung an der zu h orthogonalen Hyperebene. Wir bezeichnen mit $O(E)$ die Gruppe aller orthogonalen Transformationen $E \to E$, mit $S(E)$ die von den Spiegelungen erzeugte Untergruppe. Ist $C(U)$ die Cliffordalgebra von U, so gilt bekanntlich

$$O(U) = \{u \in \mathrm{Aut}(C(U)) / u(U) = U\}$$

ISSN 0021-8693

und daraus folgt: $O(E) = \{u \in \mathrm{Aut}(C(U))/u(E) = E\}$. Seien nun $h, w \in E$ mit $q(h), q(w) \in A$ sowie $N := 1 + b(h, w) + q(h)\,q(w) \in A^*$, der Einheitengruppe von A und sei $1 + hw \in C(U)$. Es folgt $(1 + hw)(1 + wh) = N \in A^*$, also können wir den inneren Automorphismus von $C(U)$ mit $1 + hw$ betrachten. Wir erhalten für alle $x \in E$:

$$E_w{}^h(x) := (1 + hw)\,x(1 + hw)^{-1} = N^{-1}(x + hwx + xhw + hwxwh)$$
$$= x - N^{-1} \cdot b(q(h)w + h, x)(w + q(w)h) + b(w, x)h \in E.$$

Ist speziell $q(h) = b(h, w) = 0$ so ist $E_w{}^h$ eine Eichlertransformation. Wir wollen deshalb die soeben eingeführten orthogonalen Transformationen verallgemeinerte Eichlertransformationen nennen. Die von den Spiegelungen und den verallgemeinerten Eichlertransformationen erzeugte Untergruppe von $O(E)$ sei $X(E)$. Dann gilt sicher $S(E) \subseteq X(E) \subseteq O(E)$ und wir wollen jetzt zeigen:

SATZ 1.1. *Die Voraussetzungen* (1) *und* (2) *seien erfüllt. Dann gilt*:

(a) $X(E) = O(E)$.

(b) *Ist* $t \in O(E)$, $t \equiv id \bmod pE$ *so ist* t *ein Produkt von zur* $id \bmod pE$ *kongruenten Spiegelungen und Eichlertransformationen* $E_w{}^h$ *mit* $w \in pE$.

(c) *Ist* $t \in O(E)$ *ein Produkt von Spiegelungen und verallgemeinerten Eichlertransformationen so können letztere als* E_{aw}^h *mit* $a \in A$, $h, w \notin pE$ *und* $h + pE$, $w + pE$ *linear unabhängig in* E/pE *gewählt werden.*

Beweis. Sei $t \in O(E)$, $E_t := \{x \in E/tx = x\}$ der Fixmodul von t. Ist $E_t = E$ so ist t die Identität auf E und wir sind fertig. Ist $E_t \neq E$, so wollen wir ein $s \in X(E)$ finden für das $E_{s^{-1}t}$ einen größeren Rang als E_t hat. Da $rg(E) = \dim(U)$ als endlich vorausgesetzt ist führt dieses Verfahren nach endlich vielen Schritten zum Ziel. $b(E, (t - 1)E)$ ist wegen (1) ein Ideal in A, also $b(E, (t - 1)E) = aA$ mit $0 \neq a = p^m \in A$, $m \geqslant 0$ und $m \geqslant 1$ falls $t \equiv id \bmod pE$. Seien $e, f \in E$ mit $b(e, (t - 1)f) = a$ und $i = (t - 1)f$. Es ist $Bf \not\subseteq E_t \otimes B$, also ist $rg(Af + E_t) > rg(E_t)$. Wegen (2) ist $i \in aE$ und es gilt $q(i) = -b(f, i) \in aA$. Sei $i = ah$. Dann ist $b(e, h) = 1$ und $q(h) \in a^{-1}A$. Wir unterscheiden zwei Fälle:

1. $q(h) \notin pA$. Dann ist $s_h \in X(E)$ und es gilt $s_h f = tf$ sowie für $x \in E_t$: $b(x, h) = a^{-1}(b(x, tf) - b(x, f)) = 0$, also $tx = x = s_h x$ für $x \in E_t$ und damit folgt $E_{s_h^{-1}t} \supseteq Af + E_t$. Ist sogar $q(h) \notin A$, so gilt darüberhinaus $s_h \equiv id \bmod pE$.

2. $q(h) \in A$ für $t \equiv id \bmod pE$, $q(h) \in pA$ sonst. Stets gilt $q(i) \in a^2A$. Wir betrachten die Linearform $w \to a^{-1}b(e, (t - 1)x)$. Wegen (2) gibt es ein $u \in E$ mit

$$a^{-1}b(e, (t - 1)x) = b(u, x) \qquad \text{für alle} \quad x \in E. \tag{3}$$

Es folgt $b(t^{-1}e, x) = b(e, tx) = b(e + au, x)$ und daraus $t^{-1}e = e + au$ womit

wir erhalten: $q(au) = q(t^{-1}e - e) = -b(e, (t-1)e) \in aA$, also $q(u) \in a^{-1}A$. (3) liefert $b(u, f) = 1$, $b(u, E_t) = 0$. Für $v = tu$ gilt dann $q(v) \in a^{-1}A$, $b(v, tf) = 1$ und $b(v, E_t) = 0$, also gibt es ein $w \in Au + Av$ mit $q(w) \in a^{-1}A$, $b(w, E_t) = 0$, $b(w, f) = 1$ und $b(w, tf) \in A^*$. Es ist $b(h, f) = a^{-1}b(i, f) = -a^{-1}q(i) = -aq(h) \in pA$, also sind $w + pE$ und $h + pE$ in E/pE linear unabhängig. Wir betrachten nun E^h_{aw}. Es ist $q(h)\, q(aw) \in pA$ und damit $N = 1 + b(aw, h) + q(h)\, q(aw) = 1 + b(w, tf - f) + q(h)\, q(aw) = b(w, tf) + q(h)\, q(aw) \in A^*$, also ist $E^h_{aw} \in X(E)$, $a \in pA$ falls $t \equiv id \bmod pE$ und es gilt:

$$E^h_{aw} f = f - N^{-1}b(q(h)\, aw + h, f)(aw + q(aw)h) + b(aw, f)h = f + i = tf,$$

denn es ist $b(q(h)aw + h, f) = aq(h) + b(h, f) = a^{-1}(q(i) + b(i, f)) = 0$ sowie $b(aw, f)h = ah = i$. Außerdem gilt wegen $b(h, E_t) = b(w, E_t) = 0$: $E^h_{aw}(x) = x = tx$ für $x \in E_t$, also hat $(E^h_{aw})^{-1}t$ wieder einen größeren Fixraum als t. Damit ist 1.1 bewiesen.

BEMERKUNG 1.2. *Ist $q(w) \notin pA$ oder $b(h, w) \in A^*$, so ist E^h_{aw} Produkt zweier Spiegelungen.*

Beweis. Sei $q(w) \notin pA$. Dann ist $s_w \in O(E)$. Ferner gilt in $C(U)$:

$$(1 + ahw)w = w + aq(w)h \in E,$$

denn es war $q(w) \in a^{-1}A$. Es ist $q(w + aq(w)h) = q(w)N \notin pA$, also ist auch $s_{w+aq(w)h} \in O(E)$ und es gilt: $E^h_{aw}(-s_w) = -s_{w+aq(w)h}$, also $E^h_{aw} = s_{w+aq(w)h}s_w$. Sei nun $q(w) \in pA$ und $b(h, w) \in A^*$. Dann gilt $q(w + h) \in A^*$ und es ist $(1 + ahw)(w + h) = x \in Ah + Aw$. Es gilt:

$$\begin{aligned} q(x) = x^2 &= (1 + ahw)(w + h)(1 + ahw)(w + h) \\ &= (1 + ahw)(1 + awh)(w + h)^2 \\ &= Nq(w + h) \in A^*. \end{aligned}$$

Wie oben folgt: $E^h_{aw} = s_x s_{w+h}$.

BEMERKUNG 1.3. *$F = Ah + Aw = Ah \oplus Aw$ ist ein freier direkter Summand von E mit $rg(F) = 2$.*

Beweis. $\bmod pE$ sind h, w linear unabhängig, denn $Aw + Ah + Ae$ für $b(w, w) \in A^*$ bzw. $Aw + Af + Ah + Ae$ für $b(w, w) \in pA$ ist unimodulares Teilgitter von E.

2. ERZEUGUNG DER ORTHOGONALEN GRUPPE DURCH SPIEGELUNGEN

Die folgenden Hilfssätze beschäftigen sich mit der Frage, wann $S(E) = O(E)$ gilt und wann nicht.

HILFSSATZ 2.1. *Gibt es in E einen freien direkten Summanden F mit $rg(F) = 2$ und $q(F) \subseteq pA$ und gilt außerdem $q(E) \cap A^* = \varnothing$, so ist $S(E) \neq O(E)$.*

Beweis. Sei $F = Ah \oplus Aw$, $x \in E$ mit $b(x, h) = 1$, $b(x, w) = 0$. Dann ist $E_w{}^h \in O(E)$ und es gilt $E_w{}^h x \equiv x - w \bmod pE$, während für alle Spiegelungen wegen $q(E) \cap A^* = \varnothing$ gilt: $s = id \bmod pE$, also ist $E_w{}^h \notin S(E)$.

HILFSSATZ 2.2. *Besitzt E keinen freien direkten Summanden F mit $rg(F) = 2$ und $q(F) \subseteq pA$ so ist $S(E) = O(E)$.*

Beweis. In 1.1 ist gezeigt worden, daß sich jedes $t \in O(E)$ als Produkt von Spiegelungen und verallgemeinerten Eichlertransformationen E_{aw}^h schreiben läßt. Dabei ist $F = Ah \oplus Aw$ ein freier direkter Summand mit $rg(F) = 2$. Es war $q(h) \in pA$ und nach 1.2 ist E_{aw}^h Produkt von Spiegelungen wenn entweder $q(w) \notin pA$ oder $b(h, w) \in A^*$ ist, also kann E_{aw}^h nur dann nicht Produkt von Spiegelungen sein, wenn $q(Ah + Aw) \subseteq pA$ ist.

HILFSSATZ 2.3. *Sind h, w, $x \in E$ mit $q(h)$, $q(w)$, $q(x) \in A$ sowie $N = 1 + b(h, w) + q(h)q(w) \in A^*$, $N' = 1 + b(w, h - x) + q(w)q(h - x) \in A^*$ so gilt: $E_w{}^h$, E_w^{h-x} und $E_x^{-N^{-1}(w+q(w)h)}$ sind verallgemeinerte Eichlertransformationen und es gilt $E_w{}^h = E_x^{-N^{-1}(w+q(w)h)} E_w^{h-x}$.*

Beweis. Es ist $(1 - N^{-1}(w + q(w)h)x)(1 + (h - x)w) = N'N^{-1}(1 + hw)$ wie eine direkte Rechnung in $C(U)$ zeigt. Außerdem sind $E_w{}^h$, $E_w^{h-x} \in O(E)$, also auch $E_x^{-N^{-1}(w+q(w)h)}$ und es gilt obige Beziehung.

HILFSSATZ 2.4. *Besitzt A/pA mehr als zwei Elemente und ist $q(E) \cap A^* \neq \varnothing$ so ist $S(E) = O(E)$.*

Beweis. Wegen 1.1 und 2.2 genügt es, den Fall zu betrachten, daß E einen zweidimensionalen direkten Summanden $F = Ah \oplus Aw$ mit $q(F) \subseteq pA$ besitzt und daß $t = E_{aw}^h$ mit $0 \neq a \in A$ ist. Sei $z \in E$ mit $q(z) \in A^*$ und $c \in A^*$ so, daß $cb(aw, z) \not\equiv -1 \bmod pA$ und $b(h, z) \not\equiv cq(z) \bmod pA$ ist. Das ist möglich, da A/pA mindestens vier Elemente besitzt. $x = cz$ hat dann die folgenden Eigenschaften: $q(x)$, $q(h - x) \in A^*$, $1 + b(aw, h - x) + q(aw)\, q(h - x) \in A^*$, also ist nach 2.3 mit dem dortigen $N \in A^*$: $E_{aw}^h = E_x^{-N^{-1}(aw+q(aw)h)} E_{aw}^{h-x}$. Nun ist aber für beliebiges $i \in E$ mit $q(i) \in A$ und $N' = 1 + b(i, x) + q(i)\, q(x) \in A^*$ $E_x{}^i = s_{x+q(x)i} s_x$, da $q(x + q(x)i) = q(x)N' \in A^*$ ist und da in $C(U)$ gilt: $(x + q(x)i)x = q(x)(1 + ix)$. Ebenso rechnet man leicht nach:

$$E_{aw}^{h-x} = s_{h-x} s_{h-x+q(h-x)aw} \cdot$$

Damit haben wir bewiesen:

SATZ 2.5. *Besitzt A/pA mehr als zwei Elemente so gilt $O(E) \neq S(E)$ genau*

dann, wenn es in E einen freien direkten Summanden F vom Rang zwei mit $q(F) \subseteq pA$ gibt und wenn $q(E) \cap A^* = \varnothing$ ist. Für vollkommene Restklassenkörper erhalten wir daraus:

SATZ 2.6. *Besitzt A/pA mehr als zwei Elemente und ist vollkommen so gilt stets $S(E) = O(E)$.*

Beweis. Wegen 2.5 können wir uns auf den Fall beschränken, daß E einen freien direkten Summanden $F = Ah \oplus Aw$ vom Rang zwei mit $q(F) \subseteq pA$ enthält. Da E unimodular ist folgt dann $rg(E) \geqslant 4$ und E enthält ein unimodulares Teilgitter $G = Ax \oplus Ay \oplus Ah \oplus Aw$ mit $b(x, h) = b(y, w) = 1$, $b(x, w) = b(y, h) = 0$ und so, daß $E = G \perp G^{\perp}$ ist. Wir wollen nun sehen, daß es ein $z \in G$ gibt mit $q(z) \in A^*$. Ohne Einschränkung können wir annehmen $q(x), q(y) \notin A$, denn sonst wähle man für z einen der Vektoren $x, y, x + h, y + w$. Sei $v: A \to \mathbb{Z}$ die Exponentenbewertung mit $v(p) = 1$. Gilt $v(q(x)) \not\equiv v(q(y)) \bmod 2$ so gibt es ein $n \in \mathbb{N}$ mit $q(p^n x) \in A^*$ oder $q(p^n y) \in A^*$. Ist $v(q(y)) - v(q(x)) = 2n$ und o.E. $n \geqslant 0$ so ersetze man y durch $y' = y + ap^n x$ wobei $a \in A^*$ so zu wählen ist, daß $v(q(y')) > v(q(y))$ wird. Das ist möglich, da A/pA vollkommen ist. Gilt $v(q(x)) \not\equiv v(q(y')) \bmod 2$ so verfahre man wie dort, sonst wiederhole man das Verfahren bis man zu einem u mit $q(u) \in A$ kommt. Da immer noch $b(u, w) = 1$ gilt ist dann entweder $q(u)$ oder $q(u + w)$ Einheit in A.

3. DER RESTKLASSENKÖRPER MIT ZWEI ELEMENTEN

In diesem Paragraphen sei stets $A/pA \cong F_2$, der Primkörper mit zwei Elementen. Es gilt:

HILFSSATZ 3.1. *Ist $rg(E) \leqslant 3$ oder $rg(E) \geqslant 7$ so gilt $S(E) = O(E)$.*

Beweis. Der Fall $rg(E) \leqslant 3$ folgt unmittelbar aus 2.2 und für $rg(E) \geqslant 7$ können wir ebenfalls wegen 2.2 annehmen, daß es ein $F = Ah \oplus Aw \subseteq E$ mit $q(F) \subseteq pA$ gibt und $t = E^h_{aw}$ ist. Wir wollen analog zu 2.4 und 2.6 vorgehen. Dazu benötigen wir ein $x \in E$ mit $q(h - x) \in A^*$ so daß auch

$$1 + b(aw, h - x) + q(aw)\, q(h - x) \in A^*$$

gilt. Das ist gleichbedeutend mit $q(x) \in A^*$, $b(h, x) \in pA$, $b(aw, x) \in pA$, wobei die letzte Bedingung nur für $a \in A^*$ von Bedeutung ist. Sei $E = G \perp G^{\perp}$ mit G wie in 2.6. Wir wollen in $G^{\perp}$ ein x finden mit $q(x) \in A^*$ und unterscheiden dazu die beiden Fälle $rg(E)$ ungerade und $rg(E)$ gerade. Ist $rg(E)$ ungerade, so enthält $G^{\perp}$ ein unimodulares Teilgitter $H = Au \perp (Ae + Af)$ mit $b(u, u) \in A^*$, also $q(u) \notin A$ und $b(e, f) = 1$. Ist $q(e), q(f) \in A$ so können wir für x einen der

Vektoren $e, f, e+f$ wählen. Sei also o.E. $q(e) \notin A$. Dann ist sicher $v(q(u)) \leqslant v(q(e))$, also können wir das Verfahren, das wir in 2.6 auf x, y angewandt haben auf u, e anwenden und erhalten so ein $x \in H$ mit $q(x) \in A^*$. Ähnlich verfahren wir falls $rg(E)$ gerade ist. Dann ist $rg(G^\perp) \geqslant 4$ und G enthält ein unimodulares Teilgitter $H = (Au \oplus Au') \perp (Ae \oplus Af)$ mit $b(u, u') = b(e, f)) = 1$. Wir können wieder $q(u), q(e) \notin A$ annehmen und dann mit u, e so verfahren wie im Beweis von 2.6 mit x, y. Es gibt also stets ein $x \in E$ mit $q(x) \in A^*$, $b(h, x) = b(w, x) = 0$. 2.3 liefert $E_{aw}^h = E_x^{-N^{-1}(aw+q(aw)h)} E_{aw}^{h-x}$ und wie in 2.4 ist jede der rechts stehenden verallgemeinerten Eichlertransformationen Produkt zweier Spiegelungen.

Es bleiben also die Fälle $rg(E) = 4, 5, 6$ wobei stets gilt: $E = G \perp H$ mit $G = Ax \oplus Ay \oplus Ah \oplus Aw$ und $b(x, h) = b(y, w) = 1$, $b(x, w) = b(y, h) = 0$ sowie $q(Ah \oplus Aw) \subseteq pA$. Ferner können wir uns auf $t = E_{aw}^h$ beschränken.

HILFSSATZ 3.2. *Ist $rg(E) = 5$ oder 6, so ist $t = E_{aw}^h$ sicher immer dann Produkt von Spiegelungen wenn im Fall $rg(E) = 5$ $v(2)$ gerade ist oder im Fall $rg(E) = 6$ $H \ncong Au + Au'$ mit $q(u) \notin A$, $b(u, u') = 1$, $q(u') \in pA$ ist.*

Beweis. Wie in 3.1 genügt es, wenn wir ein $z \in H$ finden mit $q(z) \in A^*$. Ist $rg(E) = 5$ so ist $H = Au$ mit $q(u) = c/2$ und $c \in A^*$ (und damit sicher $\mathrm{char}(A) = 0$) sowie $v(q(u)) = -v(2)$. Ist also $v(2)$ gerade so kann man $z = p^{2^{-1}v(2)}u$ wählen. Sei $rg(E) = 6$, also $H \cong Au \oplus Au'$ mit $b(u, u') = 1$. Sind $q(u), q(u') \in A$ oder $q(u) \notin A$ und $v(q(u))$ gerade oder $q(u') \notin A$ und $v(q(u'))$ gerade so existiert wieder ein $z \in H$ mit $q(z) \in A^*$. Sei also o.E. $q(u) \notin A$, $v(q(u))$ ungerade. Ist $q(u') \notin pA$ und $v(q(u'))$ ungerade so können wir noch annehmen $v(q(u)) \leqslant v(q(u'))$. Es folgt die Behauptung durch Abändern von u' wie in 2.6.

HILFSSATZ 3.3. *Sei $rg(E) = 5$ oder 6. Es ist $S(E) = O(E)$ außer wenn gilt: $E \cong G \perp H$ mit $rg(G) = 4$, $q(G) \subseteq A$, G enthält freien direkten Summanden F mit $rg(F) = 2$ und $q(F) \subseteq pA$ sowie: $v(2)$ ist ungerade für $rg(E) = 5$; $H \cong Au \oplus Au'$ mit $b(u, u') = 1$, $q(u) \notin A^*$, $v(q(u))$ ungerade und $q(u') \in pA$ für $rg(E) = 6$.*

Beweis. Ist $S(E) \neq O(E)$ so gibt es ein $t = E_{aw}^h \in O(E) \setminus S(E)$. Sei $F = Ah \oplus Aw$ und $G = Ax \oplus Ay \oplus Ah \oplus Aw$ wie in 2.6. Ist $q(G) \subset A$ so sind wir mit 3.2 fertig. Sei also $z_0 \in G$, $q(z_0) \notin A$ und sei $t \notin S(E)$. Dann ist $v(q(z_0))$ ungerade für alle $z_0 \in G$ mit $q(z_0) \notin A$. Existiert nämlich eines mit $v(q(z_0))$ gerade so sei $z = p^n z_0$ mit $q(z) \in A^*$. Wegen $n > 0$ ist dann $b(h, z) \in pA$, $b(w, z) \in pA$ so daß wir wie in 3.1 verfahren können und $t \in S(E)$ erhalten. Sei nun $z_0 \in G$ so, daß $v(q(z_0))$ minimal ist. Wegen $q(F) \subseteq pA$ (und $b(G, G) \subset A$) können wir $z_0 \in \{x, y\}$ wählen und wegen $t^{-1} = E_{ah}^w$ dann o.E. $z_0 = x$. 3.2 liefert, daß $u \in H$ existiert mit $q(u) \notin A$ und daß für alle diese $v(q(u))$ ungerade ist. Sei auch $u \in H$ so, daß $v(q(u))$ minimal ist. Gilt $v(q(u)) > v(q(x))$ was nur für $rg(E) = 6$ möglich ist, so gibt es ein $a \in pA$ mit $v(q(u + ax))$ gerade und negativ

oder eines mit $q(u + ax) \in A$ und in beiden Fällen wäre dann $t \in S(E)$ wie man analog zu 2.6 und 3.1 sieht. Also ist $v(q(u)) \leqslant v(q(x))$. $t \notin S(E)$ liefert wieder: Es existiert ein $a \in A$ mit $q(x + au) \in A$. Betrachtet man $G' = A(x + au) \oplus Ay \oplus F$ anstelle von G, $G'^{\perp}$ anstelle von H so kann man, falls $q(y) \notin A$ ist, obiges Verfahren nochmals anwenden. Man erhält jedenfalls ein G_a mit $q(G_a) \subseteq A$ und damit die Behauptung.

HILFSSATZ 3.4. *Sei* $E \cong E_1 \perp E_2 \perp E_3$, $E_i = Au_i \oplus Av_i$ *und* $q(u_1) \notin A$, $v(q(u_1))$ *ungerade,* $q(u_2), q(u_3) \in A^*$, $q(v_i) \in pA$ *sowie* $b(u_i, v_i) = 1$ *für* $i = 1, 2, 3$. *Dann gilt* $E_{v_3}^{v_2} \notin S(E)$.

Beweis. Sei $\bar{E} := E/pE$. Jedes $t \in O(E)$ induziert ein $\bar{t} \in \mathrm{Aut}(\bar{E})$. Wir wollen untersuchen, welche $\bar{t}$ als Bilder von Elementen aus $S(E)$ auftreten. Es gilt $\bar{s}_x = \mathrm{id}$. falls $q(x) \notin A$ ist, also brauchen wir nur $x \in E$ mit $q(x) \in A^*$ zu betrachten, denn $q(x) \in pA$ kann wegen der Unimodularität von E nicht vorkommen. Außerdem ist für $x \equiv x' \bmod pE$ natürlich $\bar{s}_x = \bar{s}_{x'}$. Sei also $x = \sum_{i-1}^{3} a_i u_i + \sum_{i-1}^{3} c_i v_i \in E$. Dann gilt:

$$q(x) - (a_1^2 q(u_1) + a_1 c_1 + a_2^2 q(u_2) + a_2 c_2 + a_3^2 q(u_3) + a_3 c_3) \in pA,$$

also liefert $q(x) \in A^*$: $a_1 \in pA$ und damit wegen $v(q(u_1))$ ungerade: $a_2^2 q(u_2) + a_2 c_2 + a_3^2 q(u_3) + a_3 c_3 \in A^*$. Es folgt $q(x) \in A^*$ genau dann, wenn $x \equiv x' \bmod pE$ ist und

$$x' \in \{u_2, u_2 + v_1, u_2 + v_3, u_2 + u_3 + v_3, u_2 + v_1 + v_3, u_2 + u_3 + v_1 + v_3,$$
$$u_3, u_3 + v_1, u_3 + v_2, u_2 + u_3 + v_2, u_3 + v_1 + v_2, u_2 + u_3 + v_1 + v_2\}$$
$$:= C \text{ ist.}$$

Es gilt also $\overline{S(E)} = \{\bar{s}_x / x \in C\}$. Wir betrachten nun den Unterraum $\bar{U} := \bar{A}\bar{u}_2 + \bar{A}(\bar{u}_3 + \bar{v}_2) + \bar{A}\bar{v}_1 \subset \bar{E}$. Dann rechnet man leicht nach, daß $\bar{U}$ unter $\overline{S(E)}$ invariant ist, hingegen gilt: $\overline{E_{v_3}^{v_2} u_2} = \bar{u}_2 + \bar{v}_3 \notin \bar{U}$.

Anmerkung. Diese Beweisführung sowie die Beweise von 3.5 und 3.7 gehen analog zu Teil 10 aus [2]. Mit diesen Vorbereitungen können wir nun auch für $A/pA = F_2$ die Moduln mit $O(E) \neq S(E)$ angeben. Es gilt:

SATZ 3.5. *Es ist* $S(E) \neq O(E)$ *genau dann, wenn gilt:* $4 \leqslant rg(E) \leqslant 6$ *und mit* E_i $i = 1, 2, 3$ *wie in* 3.4. $E \cong E_1 \perp E_2 \perp E_3$ *falls* $rg(E) = 6$ *ist;* $E \cong E_0 \perp E_2 \perp E_3$ *mit* $E_0 = Au_0$ *und* $b(u_0, u_0) \in A^*$ *sowie* $v(2)$ *ungerade falls* $rg(E) = 5$ *ist;* $E \cong E_2 \perp E_3$ *oder* $E \cong E_1 \perp E_2$ *falls* $rg(E) = 4$ *ist.*

Beweis. Ist $E \ncong E_1 \perp E_2$ so enthält E den Modul $E_2 \perp E_3$, also ist $E_{v_3}^{v_2} \in O(E)$ aber wegen 3.4 $E_{v_3}^{v_2} \notin S(E')$, wobei $E' = E_1 \perp E_2 \perp E_3$ ist und

$E \subseteq E'$. Dann ist aber erst recht $E_{v_3}^{v_2} \notin S(E)$. Außerdem liefert 3.3, daß für $5 \leqslant rg(E) \leqslant 6$ alle Moduln mit $S(E) \neq O(E)$ obige Gestalt haben, denn es ist das dortige $G \cong E_2 \perp E_3$. Sei also $rg(E) = 4$. Dann enthält E wegen 1.2 einen freien direkten Summanden F mit $rg(F) = 2$ und $q(F) \subseteq pA$, also gilt $E = G_1 \perp G_2$ mit $G_i = Ax_i + Ay_i$ und $b(x_i, y_i) = 1$, $q(y_i) \in pA$ $i = 1, 2$. Ist $q(E) \subseteq A$, so folgt $E \cong E_2 \perp E_3$ und dafür ist $S(E) \neq O(E)$ oben bewiesen. Ist $q(E) \not\subseteq A$, so sei o.E. $q(x_1) \notin A$. Dann folgt $v(q(x_1))$ ungerade analog zum Beweis von 3.3. Ist $q(x_2) \in A$, so gilt $E \cong E_1 \perp E_2$ und ebenso für $q(x_2) \notin A$, da dann auch $v(q(x_2))$ ungerade sein muß und wir wie im Beweis von 3.1 verfahren können. Sei also $E \cong E_1 \perp E_2$. Um $O(E) \neq S(E)$ zu beweisen gehen wir wie in 3.4 vor. Ist $x = a_1u_1 + a_2u_2 + c_1v_1 + c_2v_2 \in E$, so ist $q(x) \in A^*$ genau dann, wenn $a_1 \in pA$, $a_2 \in A^*$ und $c_2 \in pA$ ist. $\overline{S(E)}$ wird also von $\bar{s}_{u_2}$ und $\bar{s}_{u_2+v_1}$ erzeugt. Es folgt: $\bar{t}\bar{u}_2 = \bar{u}_2$ für alle $t \in S(E)$ wohingegen $\overline{E_{v_2}^{v_1}}\bar{u}_2 = \bar{u}_2 + \bar{v}_1$ gilt. Damit ist 3.5 bewiesen.

HILFSSATZ 3.6. *Ist A/pA vollkommen und gilt für $t \in O(E)$ $t \equiv id \bmod pE$ so ist $t \in S(E)$.*

Beweis. Mit dem schon bewiesenen können wir uns auf die Ausnahmefälle von 3.5 und wegen 1.1 und 1.2 auf $t = E_{aw}^{h}$ mit $a \in pA$, $h + pE$, $w + pE$ linear unabhängig in E/pE sowie $q(h)$, $b(h, w)$, $q(w) \in pA$ beschränken. Nun gibt es aber in jedem der Ausnahmefälle ein $x \in E$ mit $q(x) \in A^*$ und entweder $b(h, x) \in pA$ oder $b(w, x) \in pA$. Beachtet man noch $E_{aw}^{h} = (E_{ah}^{w})^{-1}$ so folgt mit 2.3 die Behauptung.

SATZ 3.7. *In den Ausnahmefällen von* 3.5 *gilt* $|O(E) : S(E)| = 2$.

Beweis. Aus 3.5 folgt $|O(E) : S(E)| \geqslant 2$. Sei wieder $\bar{E} = E/pE$, ferner $\overline{O(E)}$ das Bild von $O(E)$ in $\mathrm{Aut}(\bar{E})$, ebenso $\overline{S(E)}$. Ist $t \in O(E)$, so sei $\bar{t}$ das Bild von t in $\overline{O(E)}$. Ist für $E' \subseteq E$ $q(E') \subseteq A$ so gilt sicher $\overline{O(E')} \subseteq \overline{O(E)}$ sowie $\overline{S(E')} = \overline{S(E)}$. Wegen 3.6 müssen wir nur noch zeigen: $|\overline{O(E)} : \overline{S(E)}| \leqslant 2$. Wir behandeln die Fälle von 3.5 in etwas anderer Reihenfolge und verwenden die dortigen Bezeichnungen.

1. Fall. $E = E_2 \perp E_3$. Dann gilt $q(E) \subseteq A$ und es ist bekanntlich $|O(\bar{E}) : S(\bar{E})| = 2$.

2. Fall. $E = E_0 \perp E_2 \perp E_3$. Sei $t \in O(E)$, $tu_0 = u_0 + x$. Wäre $x \notin pE$ so würde gelten: $0 \neq \bar{x} \in \bar{E}_2 \perp \bar{E}_3$ wegen $q(u_0) = q(tu_0) \notin A$. Dann gibt es aber ein $y \in E_2 \perp E_3$ mit $b(x, y) = 1$ und es würde folgen $u_0 - b(u_0, u_0)y \in (Atu_0)^{\perp}$ und $q(u_0 - b(u_0, u_0)y) \notin A$. Es gilt also für alle $t \in O(E)$: $tu_0 \equiv u_0 \bmod pE$ woraus folgt: $\bar{t}(\bar{E}_2 \perp \bar{E}_3) = \bar{E}_2 \perp \bar{E}_3$ und das ist im 1. Fall behandelt.

3. Fall. $E = E_1 \perp E_2 \perp E_3$. Dann gilt sicher $\bar{s}_x \in \overline{S(E)}$ für $\bar{x} \in \{\bar{u}_2 + \bar{v}_1, \bar{u}_3 + \bar{v}_2, \bar{u}_2, \bar{u}_3 + \bar{v}_1, \bar{u}_2 + \bar{v}_3, \bar{u}_3\}$ und es gilt:

$$
\begin{array}{ccccccc}
\bar{u}_1 & \xrightarrow{\bar{s}_{u_2+v_1}} & \bar{u}_1+\bar{u}_2+\bar{v}_1 & \xrightarrow{\bar{s}_{u_3+v_2}} & \bar{u}_1+\bar{u}_2+\bar{u}_3+\bar{v}_1+\bar{v}_2 & \xrightarrow{\bar{s}_{u_2}} & \bar{u}_1+\bar{u}_3+\bar{v}_1+\bar{v}_2 \\
\bar{s}_{u_3+v_1}\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\bar{u}_1+\bar{u}_3+\bar{v}_1 & \longrightarrow & \bar{u}_1+\bar{u}_2+\bar{u}_3 & \longrightarrow & \bar{u}_1+\bar{u}_2+\bar{v}_2 & \longrightarrow & \bar{u}_1+\bar{v}_2 \\
\bar{s}_{u_2+v_3}\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\bar{u}_1+\bar{u}_2+\bar{u}_3+\bar{v}_1+\bar{v}_3 & \longrightarrow & \bar{u}_1+\bar{u}_3+\bar{v}_3 & \longrightarrow & \bar{u}_1+\bar{v}_2+\bar{v}_3 & \longrightarrow & \bar{u}_1+\bar{u}_2+\bar{v}_2+\bar{v}_3 \\
\bar{s}_{u_2}\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\bar{u}_1+\bar{u}_2+\bar{v}_1+\bar{v}_3 & \longrightarrow & \bar{u}_1+\bar{v}_3 & \longrightarrow & \bar{u}_1+\bar{u}_3+\bar{v}_2+\bar{v}_3 & \longrightarrow & \bar{u}_1+\bar{u}_2+\bar{u}_3+\bar{v}_2+\bar{v}_3
\end{array}
\tag{4}
$$

wobei in jeder Zeile (Spalte) dieselbe Spiegelung anzuwenden ist. Da die angegebenen Vektoren alle Klassen von Elementen $x \in E$ mit $q(x) - q(u_1) \in pA$ repräsentieren gibt es also zu $t \in O(E)$ stets ein $t_0 \in S(E)$ mit $t'u_1 := t^{-1}tu_1 \equiv u_1 \bmod pE$. Für t' gilt aber auch $t'v_1 \equiv v_1 \bmod pE$. Ist nämlich $t'v_1 = v_1 + x$ so gilt wegen $q(t'v_1) \in pA$ und $b(t'u_1, t'v_1) = 1$ sicher $\bar{x} \in \bar{E}_2 \perp \bar{E}_3$. Ist $x \notin pE$ so gibt es wieder ein $y \in E_2 \perp E_3$ mit $b(x, y) = 1$; also gilt für $z = u_1 - b(u_1, u_1)v_1 + y$: $z \in (\bar{A}\bar{t}\bar{u}_1 + \bar{A}\bar{t}\bar{v}_1)^\perp$ und das ist wegen $q(z) \notin A$ nicht möglich. Es folgt $\bar{t}'\bar{x} = \bar{x}$ für alle $\bar{x} \in \bar{E}_1$, also $\bar{t}'(\bar{E}_2 \perp \bar{E}_3) = \bar{E}_2 \perp \bar{E}_3$ und damit sind wir auch in diesem Fall fertig.

4. Fall. $E = E_1 \perp E_2$. Aus (4) und $\overline{E^{v_1}_{v_2} u_1} = \bar{u}_1 + \bar{v}_2$ folgt wie im 3. Fall, daß es zu jedem $t \in O(E)$ ein $t_0 \in S(E) \cup S(E)E^{v_1}_{v_2}$ gibt mit $t_0^{-1}tx \equiv x \bmod pE$ für alle $x \in E_1$ und damit wegen $\overline{O(E_2)} = \overline{S(E_2)}$ ebenfalls die Behauptung.

4. Nicht vollkommene Restklassenkörper

Hier wollen wir an einem Beispiel sehen, daß $O(E)/S(E)$ unendliche Ordnung haben kann. Dazu sei k ein nichtvollkommener Körper der Charakteristik zwei. Nach dem Satz von Hasse *et al.* [4] gibt es einen unverzweigten diskreten Bewertungsring A mit $\mathrm{char}(A) = 0$ und $A/2A \cong k$. Sei $c \in A$ so, daß $\bar{c} = c + 2A \in k$ kein Quadrat in k ist und sei $E = E_1 \perp E_2$ mit $E_i = Au_i \oplus Av_i$ $(i = 1, 2)$ ein quadratischer A-Modul mit $q(u_1) = 2^{-1}$, $q(u_2) = 2^{-1}c$, $q(v_i) = d_i \in 2A$ und $b(u_i, v_i) = 1$ $(i = 1, 2)$. Dann gilt $q(E) \cap A^* = \varnothing$, denn für $x = \sum_{i=1}^{2} (a_iu_i + b_iv_i) \in E$ ist $q(x) = 2^{-1}(a_1^2 + ca_2^2) + \sum_{i=1}^{2} (a_ib_i + d_ib_i^2)$. Sind $a_1, a_2 \in 2A$, so folgt $q(x) \in 2A$ während sonst $(0, 0) \neq (\bar{a}_1, \bar{a}_2) \in k^2$ gilt. Nun ist aber $\overline{b(x, x)} = \bar{a}_1^2 + \bar{c}\bar{a}_2^2$ und diese quadratische Form ist über k anisotrop, also gilt in diesem Fall stets $b(x, x) \in A^*$, also $q(x) \notin A$. Wie in 2.1 folgt für alle $s \in S(E)$: $s \equiv id \bmod 2E$, wohingegen für die verallgemeinerten Eichlertransformationen $E^{av_1}_{bv_2}$ mit $a, b \in A$ gilt: $E^{av_1}_{bv_2} \equiv id \bmod 2E$ genau dann, wenn $ab \in 2A$ ist. Sonst gilt $E^{av_1}_{bv_2} = E^{ab^{-1}v_1}_{v_2}$ und $E^{av_1}_{v_2} E^{bv_1}_{v_2} \equiv E^{(a+b)v_1}_{v_2} \bmod 2E$. Wir

erhalten also $\{\overline{E^{av_1}_{bv_2}}/a,\ b \in A\} \cong k$ und damit insbesondere $O(E)/S(E)$ ist nicht endlich.

Referenzen

1. M. Kneser, "Witts Satz für quadratische Formen über lokalen Ringen," Nachrichten der Akademie der Wissenschaften, Göttingen, 1972.
2. O. T. O'Meara and B. Pollak, Generation of local integral orthogonal groups, *Math Z.* **87** (1965), 385–400.
3. O. T. O'Meara and B. Pollak, Generation of local integral orthogonal groups. II, *Math. Z.* **93** (1966), 171–188.
4. O. Teichmüller, "Diskret bewertete perfekte Körper mit unvollkommenem Restklassenkörper," *J. Reine Angew. Math.* **176** (1937), 141–152.